

DETAILED ACTION

1. Claims 1-4 are pending in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Savage (US Pat. 4,032,764) in view of Rajski et al (hereafter Rajski)(US Pub. 2002/0016806).

4. **As to claims 1 and 3**, Savage discloses a pseudorandom number generator for generating a pseudorandom number sequence of a predetermined bit length (column 1, lines 20-25), comprising:

A first linear feedback shift register having m steps of shift registers to provide a bit string of a predetermined bit length (column 1, line 45-column 2, line 2);

An initial value generator to generate, according to predetermined conditions, initial values for the respective shift registers of the first linear feedback shift register

and supply the initial values to the first linear feedback shift register (column 3, lines 64-68);

A polynomial coefficient generator to generate, according to predetermined conditions, coefficients of a characteristic polynomial (column 4, lines 5-46);

A pseudorandom output unit to generate the pseudorandom number sequence of the predetermined bit length by carrying out bit by bit logical operations on the bit string provided by the first linear feedback shift register and output the pseudorandom number sequence (column 4, lines 16-68).

5. Savage does not disclose a second linear feedback shift register having n steps of shift registers to provide a bit string of a predetermined bit length; supply the initial values to the second linear feedback shift register; supply coefficients to the second linear feedback shift register; a primitive polynomial memory to store a plurality of primitive polynomials with identification information representative of the primitive polynomials, one of the primitive polynomials serving as a characteristic polynomial of the first linear feedback shift register; a primitive polynomial selector to select according to predetermined conditions, one of the primitive polynomials stored in the primitive polynomial memory and supply coefficients of the primitive polynomial as coefficients of a characteristic polynomial to the first linear feedback shift register.

However, Rajski discloses a second linear feedback shift register having n steps of shift registers to provide a bit string of a predetermined bit length ([0031]); supply the initial values to the second linear feedback shift register [0002]); supply coefficients to

the second linear feedback shift register ([0009]); a primitive polynomial memory to store a plurality of primitive polynomials with identification information representative of the primitive polynomials, one of the primitive polynomials serving as a characteristic polynomial of the first linear feedback shift register (memory element- [0031]); a primitive polynomial selector to select according to predetermined conditions, one of the primitive polynomials stored in the primitive polynomial memory and supply coefficients of the primitive polynomial as coefficients of a characteristic polynomial to the first linear feedback shift register ([0031]-[0032]).

6. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Savage by implementing the LFSR techniques using a primitive polynomial, as taught by Rajski, for the benefit of providing shorter feedback connections and lower levels of logic.

Allowable Subject Matter

7. Claims 2 and 4 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Pat. 5,258,936 – Method and apparatus for generating pseudorandom numbers

US Pat. 5,974,443 – High speed M-sequence generator

US Pat. 6,188,714 – Parallel M-sequence generator circuit

US Pub. 2007/0174374 – Pseudorandom number generator

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL YAARY whose telephone number is (571)270-1249. The examiner can normally be reached on Mon-Fri 9 a.m.-5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lewis Bullock can be reached on 571-272-3759. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. Y./
Examiner, Art Unit 2193

/Lewis A. Bullock, Jr./
Supervisory Patent Examiner, Art Unit 2193